# United States Senate

WASHINGTON, DC 20510

March 4, 2026

Mr. Dario Amodei
Chief Executive Officer
Anthropic PBC
548 Market St
San Francisco CA 94104

Mr. Sundar Pichai
Chief Executive Officer
Google LLC
1600 Amphitheatre Pkwy
Mountain View CA 94043

Mr. Sam Altman
Chief Executive Officer
OpenAI LLC
1455 3rd Street
San Francisco CA 94158

Mr. Elon Musk
Chief Executive Officer
x.AI Corp.
1450 Page Mill Road
Palo Alto, CA 94304

Dear Mr. Amodei, Pichai, Altman, and Musk:

I write to seek information about your companies' policies and practices regarding the facilitation of warrantless domestic surveillance and other abuses of government power by both the U.S. and foreign governments.

As you know, the Secretary of Defense announced on February 27, his intention to designate Anthropic a "Supply-Chain Risk to National Security," ending its government contracts and requiring other Department of Defense (DOD) contractors to cease their use of the company's products, after the breakdown of negotiations between DOD and the company. According to press reports, the dispute was the result of Anthropic's refusal to allow DOD to use the company's technology to collect and analyze bulk data on Americans, such as geolocation and web browsing data, purchased without any court approval under the "data broker loophole."

In short, this dispute seems to be about whether or not the most advanced AI companies in the world will allow government customers to use their products to engage in practices that may be technically legal, but that violate privacy, undermine democracy or threaten human rights. While the major AI companies are apparently willing to allow their products to be used to review domestic surveillance data obtained with court approval, Anthropic reportedly drew the line at warrantless surveillance exploiting the data broker loophole. As Dario Amodei, Anthropic's CEO, noted in a February 26 public statement, "[t]o the extent that such surveillance is currently legal, this is only because the law has not yet caught up with the rapidly growing capabilities of AI." Mr. Amodei specifically cited U.S. government agencies' warrantless purchase of location data, web browsing records, and other sensitive information from data brokers. As Mr. Amodei stated, "powerful AI makes it possible to assemble this scattered, individually innocuous data into a comprehensive picture of any person's life—automatically and at massive scale."

OpenAI announced a deal with DOD on February 28, which the company described on its website as banning the use of the company's products for "mass domestic surveillance." But the contractual language that the company published merely prohibited DOD from using the companies' products in violation of several federal laws and other policies, none of which prohibit surveillance by purchasing and analyzing data through the data broker loophole. After public criticism, OpenAI announced on March 2, that it had amended its agreement with DOD to prohibit "domestic surveillance of U.S. persons and nationals." The agreement apparently notes that the "Department understands this limitation to prohibit deliberate tracking, surveillance, or monitoring of U.S. persons or nationals, including through the procurement or use of commercially acquired personal or identifiable information." OpenAI further said that any use of the company's products by DOD intelligence agencies, such as the National Security Agency, would require a new agreement. It remains unclear how effective this language will be in practice, but there are several reasons to be concerned. For one, DOD under this Administration has proven itself to be an unreliable counterparty. It's unclear how much contractual language will stop DOD from misusing OpenAI software, especially language that legal experts have already argued is insufficient to turn legal violations into contractual breaches. Further, "intentional" and "deliberate" are malleable terms that will likely not stop DOD from surveilling Americans. In other contexts, the government has collected information on a global scale and claimed that collection of Americans' communications is "incidental" rather than "intentional" and "deliberate."

These concerns are not theoretical. My oversight, press investigations, and whistleblower reports have revealed that multiple Department of Defense components have purchased Americans' location data and internet browsing records. The data broker X-Mode Social confirmed to my office that it sold domestic location data to U.S. military customers, via defense contractors. The press reported that this data broker was collecting data from smartphone apps, including popular Muslim prayer apps. The Defense Intelligence Agency confirmed to my office that it purchased domestic location data. Public records for a no-bid contract awarded by the Office of Naval Intelligence justified the purchase of location data because the data broker also offered personal information associated with the tracked smartphone owners, including age, gender, languages spoken, and interests – "e.g., music, luxury goods, basketball."

Public contracting records also revealed that the Defense Counterintelligence and Security Agency purchased netflow data, which is a type of internet browsing data, and the Army and U.S. Cyber Command had contracts with the same data broker. A government whistleblower also revealed that the Naval Criminal Investigative Service purchased netflow data. Then-Director of the National Security Agency (NSA) Paul Nakasone also confirmed in an unclassified letter to me on December 1, 2023, that NSA purchases and uses wholly domestic netflow data. General Nakasone has since retired from government service and is now on OpenAI's Board of Directors.

The purchase of domestic location and internet browsing data is not limited to DOD. The Internal Revenue Service, Federal Bureau of Investigation, Drug Enforcement

Administration, Secret Service, and Customs and Border Protection have all also purchased phone location data and/or internet browsing data. On March 3, 2026, I led a letter, along with 71 Congressional Democrats, to the Department of Homeland Security Inspector General, requesting a review of Immigration and Customs Enforcement's purchase of location data. In addition, state and local law enforcement agencies have also purchased location data from data brokers. An investigation by the Associated Press using documents obtained by the Electronic Frontier Foundation uncovered over 40 contracts between nearly two dozen agencies and the data broker Fog Data Science. In addition, the same controversial data broker to whom the Office of Naval Intelligence and ICE awarded no-bid contracts also sold location data to the Texas State Police.

While federal law does not currently include an explicit prohibition on the government buying Americans' location data without a warrant, it is already illegal for data brokers to sell this data to the government. Consumers must explicitly consent to how their data will be used. It is not enough for an app developer to include fine print that app data will be sold or to obtain general consent to access location data. Through its recent cases against Venntel, Mobilewalla, and X-Mode Social, the Federal Trade Commission made it clear that it is an unfair business practice, in violation of Section 5 of the FTC Act, for data brokers to sell location data to the government that was obtained without consumer consent.

Merely requiring your government customers to use your products in compliance with the law is not a meaningful protection against abuse, both because Congress has failed to pass a meaningful privacy law since 1986 and because federal and state laws criminalize activities that are legal or widely accepted in other parts of the nation, including obtaining an abortion, gender-affirming care, using recreational cannabis and more. Moreover, commitments against "bulk" or "mass" surveillance are not sufficient when this Administration is willing to engage in targeted surveillance of the President's critics and political opponents.

Given this Administration's disregard for the law and its weaponization of government resources against the President's perceived enemies, every American should be deeply concerned by the prospect that the Trump Administration will abuse powerful AI technology to conduct domestic surveillance. Donald Trump and his Republican enablers in Congress will not remain in power forever, and as soon as Democrats are back in power, we will hold responsible the companies that enabled the abuses committed by his Administration. In order to facilitate oversight and an informed debate about the need to regulate government use of AI, please confirm in writing, by April 3, 2026, whether your company contractually prohibits your government customers — in the U.S. and overseas — from using your products for the following purposes:

1. To analyze commercial location data that was sold to the government or government contractors in violation of the FTC Act.
2. To analyze commercial web browsing, real time bidding, or netflow data that was sold to the government or government contractors in violation of the FTC Act.

3. To analyze data acquired through mass or bulk domestic collection conducted by government agencies or at the direction of government agencies.
4. To analyze data acquired through mass or bulk foreign intelligence collection conducted by government agencies or at the direction of government agencies, to the extent such collection includes information of or about U.S. persons.
5. To identify new targets for domestic surveillance or surveillance of U.S. persons.
6. To conduct domestic hacking operations or hacking operations targeting U.S. persons.
7. To facilitate the enforcement of U.S. immigration laws.
8. To facilitate the collection, analysis, dissemination or use in criminal proceedings of information related to protests or the recording, documentation, and distribution of information related to the activities of law enforcement or immigration enforcement agencies.
9. To facilitate the enforcement of U.S., state or foreign laws criminalizing abortion.
10. To facilitate the enforcement of U.S., state or foreign laws criminalizing gender affirming care.
11. To facilitate the enforcement of foreign countries' laws criminalizing blasphemy, criticism of the government or head of state (including lèse-majesté laws), or homosexuality.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden
United States Senator